Math 521A Exam 2 Solutions

Nov 10, 2011

1. (10 pts) Let k and n be positive integers. For a fixed $m \in \mathbb{Z}$, define the formula $F : \mathbb{Z}_n \to \mathbb{Z}_k$ by $f([x]_n) = [mx]_k$, for $x \in \mathbb{Z}$. Show that f defines a function if and only if $k|mn$.

   Suppose $k|mn$. We need to show f is well-defined, i.e. if $[x]_n = [y]_n$ then $f([x]_n) = f([y]_n)$. So suppose $[x]_n = [y]_n$. Then $x \equiv y \pmod{n}$, hence $x - y = nt$ for some $t \in \mathbb{Z}$, hence $m(x-y) = mnt$. Since $k|mn$, $mn = kq$ for some $q \in \mathbb{Z}$. Hence $m(x-y) = kqt$, hence $mx \equiv my \pmod{k}$, hence $[mx]_k = [my]_k$, hence $f([x]_n) = f([y]_n)$.

   Conversely, suppose $k \nmid mn$. Notice $[0]_n = [n]_n$. But $k \nmid (mn - 0)$, hence $f([n]_n) = [mn]_k \neq [m0]_k = f([0]_n)$. So f is not well-defined.

2. (10 pts) Let $f : A \to B$ and $g : B \to C$ be functions. Prove that if $g \circ f$ is onto then g is onto.

   Suppose $g \circ f$ is onto. Since $f(A) \subseteq B$ and $g(B) \subseteq C$,
   $$C = g \circ f(A) = g(f(A)) \subseteq g(B) \subseteq C.$$
   So $g(B) = C$. Hence g is onto.

3. (10 pts) Let $f : A \to B$ be a function. Prove that f is onto if and only if there exists a function $g : B \to A$ such that $f \circ g = 1_B$.

   Suppose f is onto. Then for all $y \in B$ there is an $x \in A$ such that $f(x) = y$. Define $g : B \to A$ as follows. For each $y \in B$, choose an $x \in A$ such that $f(x) = y$ and let $g(y) = x$. To see that $f \circ g = 1_B$, let $y \in B$, and note that $g(y)$ is an element $x \in A$ such that $f(x) = y$. Hence $f \circ g(y) = f(g(y)) = y$.

   Conversely, suppose there is $g : B \to A$ such that $f \circ g = 1_B$. Since 1_B is obviously onto, g must be onto by problem 2.

4. (10 pts) Let $x, y \in \mathbb{Z}^+$ such that $x|y$. Prove that $\phi(x)|\phi(y)$. (Hint: look at the prime factorizations.)

   Suppose $x|y$. Let $x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of x with distinct primes $p_1, \ldots, p_k$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}^+$. Then $x|y$ implies $y = p_1^{\beta_1} \cdots p_n^{\beta_n}$ with $\beta_1, \ldots, \beta_n \in \mathbb{Z}^+$, and $k \leq n$ and $\alpha_i \leq \beta_i$ for $1 \leq i \leq k$. So
   $$\phi(x) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1) \mid p_1^{\beta_1 - 1}(p_1 - 1) \cdots p_n^{\beta_n - 1}(p_n - 1) = \phi(y).$$

5. (5 pts each)
   (a) State the definition of a one-to-one function and an onto function.

   See Definition 2.1.4.

   (b) Give an example of a function that is one-to-one but not onto.

   See Definition 2.1.4.

   (c) Give an example of a function that is onto but not one-to-one.

   The function $f : \mathbb{R} \to \mathbb{R}^{\geq 0}$ is $f(x) = x^2$. Since for all $y \geq 0$, $\sqrt{y}$, and $f(\sqrt{y}) = \sqrt{y}^2 = y$, f is onto. But $f(-1) = 1 = f(1)$, so f is not one-to-one.

6. (5 pts) Prove that if a function $f : S \to T$ has an inverse, then this inverse is unique.

Suppose $g, h : T \to S$ are both inverses of f. Then

$$h = 1_S \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ 1_T = g$$

by the associativity of function composition.

7. (10 pts) **Extra credit problem.** In problem 3, you proved that if $f : A \to B$ is an onto function, then there exists a function $g : B \to A$ such that $f \circ g = 1_B$. Such a g is called a *right inverse* of f. Prove that right inverses need not be unique by constructing an example of a function $f : A \to B$ and two different functions $g, h : B \to A$ such that both g and h are right inverses of f.

By problem 3, such a function f must be onto. Consider the function f from problem 5(c). Let $g, h : \mathbb{R}^{\geq 0} \to \mathbb{R}$ be defined by $g(y) = \sqrt{y}$ and $h(y) = -\sqrt{y}$. Then

$$f \circ g(y) = f(\sqrt{y}) = \sqrt{y}^2 = y$$

and

$$f \circ h(y) = f(-\sqrt{y}) = (-\sqrt{y})^2 = y.$$

So $f \circ g = 1_{\mathbb{R}^{\geq 0}}$ and $f \circ h = 1_{\mathbb{R}^{\geq 0}}$.